КОД безопасности

Континент TLS

Система обеспечения защищенного удаленного доступа к веб-приложениям с использованием алгоритмов шифрования ГОСТ

- Централизованное управление кластером TLS-шлюзов
- Управление и мониторинг осуществляется через веб-интерфейс, доступный из Edge, Chrome и Яндекс
- Лицензирование по одновременному, а не общему количеству удаленных пользователей
- Система разграничения прав удаленных пользователей с помощью портала приложений
- Интеграция с Active Directory, SIEM-системами и WAF
- Высокая производительность – до 152 000 одновременных подключений

Возможности

Шифрование

- Криптографическая защита HTTPS-трафика по протоколу TLS.
- Поддерживаемые криптоалгоритмы:
  - Шифрование информации производится по алгоритму ГОСТ 28147–89;
  - Расчет хэш-функции по алгоритму ГОСТ Р 34.11– 2012;
  - Формирование и проверка электронной подписи осуществляются в соответствии с алгоритмом ГОСТ Р 34.10–2012.
- Поддерживаемые протоколы:
  - TLS v1.0;
  - TLS v1.2.
- Возможность работы с различным клиентским ПО:
  - Континент TLS Клиент и ZTN Клиент:
    - Поддержка туннелирования TCP-трафика через протокол TLS.
  - КриптоПро CSP и Валидата CSP:
    - Работа пользователя в браузере Edge и Яндекс Браузер.
  - Любой другой клиент, соблюдающий спецификацию TLS.

Сетевые возможности

- Сокрытие защищаемых серверов (обратный прокси-сервер):
  - К каждой сессии пользователя может быть добавлен произвольный идентификатор.
- Работа в режиме кластера с балансировкой нагрузки:
  - Неограниченное линейное масштабирование производительности.
- Блокировка неиспользуемых портов.

Режимы работы

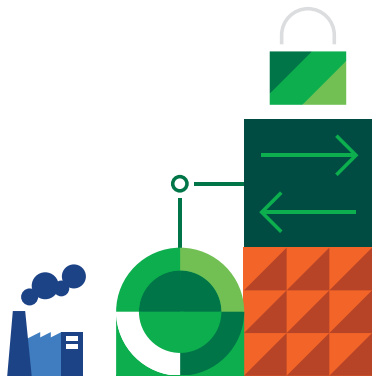
- Шифрование HTTP/HTTPS-трафика.
- Туннелирование произвольного TCP-трафика через протокол TLS.
- Публикация приложений на портале.
- Автоматическое перенаправление с HTTP на HTTPS.

Контроль доступа к защищаемым ресурсам

- Идентификация и аутентификация пользователей по сертификатам открытых ключей стандарта x.509v3 (ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012).
- Обоюдная аутентификация пользователя и сервера в процессе установки защищенного соединения.
- Проверка сертификатов ключей по спискам отозванных сертификатов (CRL).
- Автоматическая загрузка и обновление Trust-service Status List (TSL).
- Интеграция с Active Directory при работе сервера удаленного доступа в режиме портала приложений:
  - Аутентификация пользователя по имени и паролю AD;
  - Предоставление доступа к приложениям на основе принадлежности пользователя к структурному подразделению.
- NTLM аутентификация для ресурсов.
- Single-Sign-On в приложениях портала.
- Интеграция с сервисом auth.as и multifactor.ru
- Механизм просмотра и перевыпуска сертификатов кластера.
- Разграничение доступа к защищаемому ресурсу по корневому сертификату и по полям сертификата пользователя.
- Возможность управления списком разграничения доступа к ресурсам HTTPS-прокси с помощью текстового файла средствами веб-управления.

Управление и мониторинг

- Веб-интерфейс для управления и мониторинга.
- Интеграция в SIEM-систему по протоколу syslog.
- Регистрация событий информационной безопасности, связанных с работой Континент TLS Клиент.
- Поддержка утилит для сбора статистики.



Сценарии применения

Высоконагруженный портал государственных услуг

Результат:

- Минимизированы затраты на построение и эксплуатацию комплексной системы защищенного доступа к порталу государственных услуг.
- Повышена производительность приложения за счет переноса подсистемы шифрования трафика на отдельное устройство.

Система удаленного доступа к ресурсам предприятия

Результат:

- Организован доступ удаленных пользователей к внутренним веб-приложениям.
- Обеспечено разграничение доступа удаленных пользователей к различным веб-приложениям.
- Обеспечен доступ пользователей к корпоративным ресурсам с помощью толстых программных клиентов (терминалов, клиентов ERP-систем и т.д.).

Соответствие требованиям регуляторов

Результат:

- Информационная система приведена в соответствие требованиям приказа ФСТЭК России № 17 (ИАФ, УПД, ЗИС, РСБ, ОЦЛ, ОДТ, ЗТС).
- Минимизированы затраты на встраивание сертифицированной криптографии в приложения, к которым осуществляется удаленный доступ.
- Минимизированы риски, связанные с невыполнением требований регуляторов.

Модельный ряд

Характеристики	IPC-R50	IPC-R300	IPC-R550	IPC-R800	IPC-R1000	IPC-R3000	IPC-3000
Формфактор	Настольный	1U	1U	1U	1U	1U	1U
Производительность в режиме HTTPS-прокси, Мбит/с	до 600	до 600	до 1 300	до 2 400	до 2 050	до 2 500	до 5 700
Количество одновременных подключений	до 27 000	до 25 000	до 52 100	до 96 000	до 111 500	до 152 000	до 109 000
Интерфейсы RJ-45 (медь UTP)	4x 10/100/1000 BASE-T RJ45	4x 10/100/1000 BASE-T RJ45 2x Combo 1G RJ45/SFP	4x 10/100/1000 BASE-T RJ45 2x Combo 1G RJ45/SFP	8x 10/100/1000 BASE-T RJ45	8x 10/100/1000 BASE-T RJ45	8x 10/100/1000 BASE-T RJ45	1x 10/100/1000 BASE-T RJ45
Интерфейсы оптические	1x 1G SFP	2x 10G SFP+	2x 10G SFP+	4x 10G SFP+	4x 10G SFP+	8x 10G SFP+	4x 10G SFP+
Сделано в России	●	●	●	●	●	●	–

Сертификаты

Континент TLS Сервер

ФСБ России
Версия 2.6 – СКЗИ класса КС1/КС2/КС3 (Q2 2024)
Версия 2.2 – СКЗИ класса КС2/КС3

ФСТЭК России
Версия 2.5 – УД4, ТУ

Техническая поддержка

Техническая поддержка продуктов линейки «Континент» может осуществляться как напрямую, силами специалистов компании «Код Безопасности», так и через авторизованных партнеров.
В случае технической поддержки через партнера, партнер обеспечивает первую линию технической поддержки, а в случае сложных вопросов обращается в службу технической поддержки вендора.

Каталог услуг	Пакет поддержки			
	Базовый	Стандартный	Расширенный	VIP
Способ обращения в ТП	e-mail	веб-портал, e-mail	телефон, веб-портал, e-mail	
Приоритет	Низкий	Средний	Высокий	Наивысший
Консультирование по установке и использованию продукта	●	●	●	●
Доступ к Базе знаний	●	●	●	●
Доступ к пакетам обновлений	●	●	●	●
Прием предложений по улучшению продукта	●	●	●	●
Работа над инцидентами в режиме 8x5 (рабочие дни МСК 10:00–18:00)	●	●	●	●
Регистрация и контроль обращений на веб-портале		●	●	●
Работа над критичными инцидентами в режиме 24x7			●	●
Консультирование по дополнительному функционалу продукта			●	●
Выделенный инженер (для проведения работ)				●
Присутствие инженера на площадке заказчика				●

О компании «Код Безопасности»

Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

+7 (495) 982-30-20 (многоканальный) **info@securitycode.ru** **www.securitycode.ru**